STATEMENT OF THE HONORABLE CLAY JOHNSON III
DEPUTY DIRECTOR FOR MANAGEMENT
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE COMMITTEE ON GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES
June 8, 2006

Good morning, Mr. Chairman and Members of the Committee. Thank you for inviting me to speak about the adequacy of existing laws, regulations, and policies regarding privacy, information security, and data breach notification.

Unfortunately, I am here today in the wake of an unprecedented security breach causing the loss of personal data concerning millions of people. Clearly we have a problem. Losing any type of government data is bad enough, but losing personal data is especially troubling as it undermines the public's trust and confidence in our ability to protect them as individuals and keep them from harm.

As your invitation requested, I will describe our review of existing laws and policies, the lessons we have learned from the recent incident and steps for improving our response in the future. You will note the steps we are taking include a focus on better understanding how security programs are actually performing to help avoid breaches in the first place.

Over the past several weeks since the incident, we have reexamined the law and policies designed to prevent problems such as this. We have looked for weaknesses in the policies themselves and in our oversight and measurement of agency performance in implementing them. While we believe the law and policies are generally sound and this incident would not have occurred had elementary and long-standing security procedures been followed, this is a hollow victory and we are left with the same unacceptable results – a breach placing the data concerning millions of people at risk and from which each individual may have to recover.

Our review has identified four specific, but related issues. First, the recent incident makes painfully obvious a long-known security risk – a single trusted individual can mistakenly or intentionally and very quickly, undo all of the sophisticated and expensive controls designed to safeguard our information and systems from attack. To safeguard against this risk, the agencies themselves must be held accountable for implementing existing policies such as segregating personnel duties so one person cannot cause such damage.

Second, good security and privacy are shared responsibilities. As you know, within a framework of laws developed by Congress and through direction from the President, the Office of Management and Budget (OMB) develops policies for and oversees agencies' programs to protect security and information privacy. Agencies are responsible for implementing the policies based upon the risk and magnitude of harm that would result from a breach in their security, ensuring their programs are managed to

requirements and schedules for lower impact incidents. Also, to ensure a more timely picture of all agencies' operational security, I have directed my staff to work with the Department of Homeland Security, the Chief Information Officers Council, and Senior Agency Officials for Privacy to identify the appropriate level of detail and a schedule for distributing a periodic government-wide incident report to agency officials, Inspectors General, and other interested parties such as the Government Accountability Office. This may be a quarterly report – our current annual report to Congress is not timely enough.

At my direction, Senior Agency Officials for Privacy are now reviewing the effectiveness of their security programs and will report to OMB their findings early this fall with their agency's annual reports under the Federal Information Security Management Act. These reports will help us identify the extent to which additional actions are necessary.

I also would like to mention longer-term steps we are taking to increase the security of our sensitive information, computer systems, facilities, and employees. In response to an August of 2004 Presidential directive, OMB led the development of a common identification standard for several million Federal employees and contractors. This directive requires all Executive branch agencies to conduct background checks on their employees and contractors before issuing them permanent government identification. The agencies are now conducting these checks and in October of this year, will begin issuing new identification cards. These cards have built-in security features to control access to government computer systems and the government's physical facilities.

I have outlined above a number of actions we are taking to demonstrate the Administration takes its information privacy and security responsibilities very seriously. These will help prevent a recurrence of an incident such as we just experienced, permit us to better respond if prevention fails, and provide us a more complete and timely view of the security performance of the agencies. Agencies spend more than $4.5 billion each year on controls to protect information and computer systems and we will use the budget process to ensure this money is wisely spent and re-emphasize new spending on information technology will not be approved if sound security is not already in place for existing systems and programs. We are prepared to take more action as necessary and I look forward to working with you to improve our security and privacy programs and welcome any suggestions you have.